

# You've got mail – but is it safe?

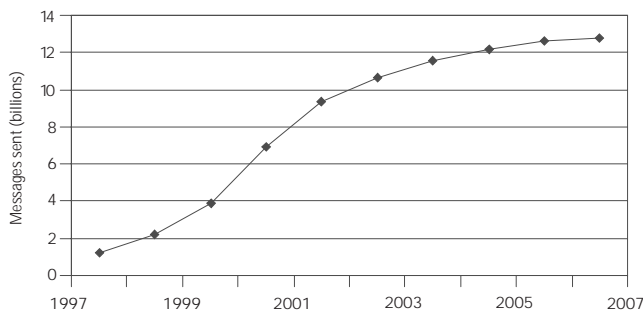
A Sophos positioning paper

September 2005

The challenges faced by organizations in maintaining information and email flow while protecting business information and client confidentiality have become ever more complex. The days are long gone when it was sufficient simply to protect the endpoint with anti-virus software and put a firewall and virus protection at the gateway. This paper focuses on the security threat that email poses to businesses. It highlights the increasingly internal nature of the threat and discusses the technologies and techniques used to combat it. The paper demonstrates how the PureMessage® product line provides a consolidated solution for email security, complementing the protection provided by Sophos Anti-Virus® at the endpoint.

## Email in a business

Email is now an indispensable business tool and its use is forecast to continue to grow, as Figure 1 shows. This growth will bring with it an increase in the number and types of threat as virus and spam writers continue to join forces to exploit network vulnerabilities for financial reward.



Source: Meta Group, Enterprise approaches to email hygiene, August 2004

Figure 1: Person-to-person messages per day

While most organizations have experienced dramatic growth in their email infrastructure, many have not seen a corresponding increase in email security – even though email is already the number one source of security threats for organizations. Over 90 percent of viruses spread via email while spam represents 60-80 percent of email volume.

*"...as the importance of email increases, the threats to the stability of the system are accelerating."*

Meta Group: Enterprise approaches to email hygiene, August 2004

## The email threat environment

Email protection tends currently to be focused on the gateway, although, as figure 2 shows, there are in reality many points of vulnerability in an email system. This can leave a network exposed to a host of email-related threats that either bypass or foil the gateway defenses, particularly if the gateway protection is itself fragmented with different vendors' anti-spam, anti-virus and policy enforcement software.

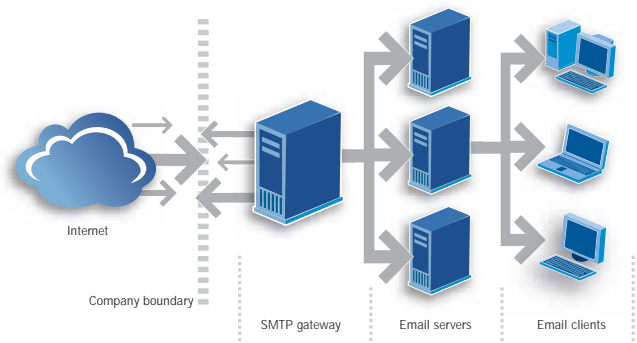


Figure 2: The multiple points of vulnerability in an email system

## At the gateway

As networks increase in size and complexity and email use grows, more points in the system become vulnerable. The gateway remains the place that the more obvious threats can strike and where email protection "traditionally" sits, providing protection against threats such as inbound spam and phishing

attacks, viruses, denial of service (DoS) attacks and directory harvest attacks (DHAs). It is also at the gateway that offensive and other inappropriate inbound emails are blocked before they can reach the corporate servers.

The growth in email has also led to increased risk of information leaving an organization which might compromise intellectual property, regulatory compliance or competitive advantage, or simply damage a company's reputation. Outbound content scanning, the policies associated with it and its implementation and management, are some way behind inbound scanning in terms of corporate investment. However, outbound scanning is an emerging issue for network administrators.

### Inside the gateway

In addition to the many security threats that a business faces at the gateway, there are an increasing number of threats that challenge email security from inside the boundary.

#### *Internal virus propagation*

Malware originating at the endpoint through, for example, instant messages or USB drives, can cause significant damage to a network from within. Effective workgroup protection can stop the propagation of viruses by detecting them in messages sent by an infected host. Within the context of the email system, the endpoint is the final line of defense.

---

*"An infected laptop could be more of a danger to [a] company's network than outside hackers – since 40 to 60 percent of the \$45 billion worth of virus and Trojan attacks annually in North America now originate on the inside."*

Vancouver Sun, 25 May 2004

---

Today's hybrid threats combine the characteristics of worms, spam and viruses. The Bofra mass-mailing worm, for example, has the appearance of being spam but its end result is a viral payload. However, the virus is not in the email (but attacks through a web link to an infected computer) and so email gateway anti-virus solutions are ineffective. Although spam filters should block the threat (and indeed Sophos PureMessage does) the only guaranteed way to catch the malicious code associated with this type of threat is through endpoint protection.<sup>1</sup>

#### *Infected email stores*

Malware can remain dormant in stored email attachments, posing a threat to the wider network long after they enter the

organization. Regular scanning of email stores can ensure old viruses are not lying unsuspected in public folders or undelivered messages.

#### *Leaking of information*

Phishing attacks can trick users into entering confidential information into fake websites. More mundanely, users can simply email information outside the company inappropriately. Spam filters can block phishing attacks, while robust email policy enforcement can ensure content security.

#### *Hijacked computers*

Desktops, laptops, and notebooks (i.e. the email clients) can be infected by an email-borne Trojan or worm and used as "zombie" computers in order to send spam or viruses to outside organizations or to launch DoS attacks on their websites. Sophos estimates that up to 50 percent of spam originates from hijacked computers, many of them within the networks of legitimate organizations, and this figure looks likely to rise. Desktop anti-virus software will detect malware attempting to turn computers into zombies. If, however, for some reason an organization does get added to a public list of servers known to send spam – domain name server blacklists (DNSBLs) – its ability to send and receive email is impeded and its reputation is at risk of being damaged.

### The security industry's position

In light of the different ways in which email can compromise an organization, the gateway email hygiene model is now beginning to look incomplete. This remains true even where security vendors are offering protection across protocols other than SMTP, such as IMAP and POP3, and where the problems of securing outbound email are being addressed through encryption products.

In addition to providing only partial coverage of the vulnerable points in a network, many gateway-centric solutions also suffer from system management flaws. These are a result both of the rapid technological evolution and of the tendency for vendors to bolt new pieces onto older architectures, rather than tightly integrating new functionality into a consistent administration model.

In a similar way, the technology itself is challenged. The mainstay for most anti-spam vendors has been "traffic profiling" which uses sender reputation filtering to compare

---

*Relying on pure-play gateway vendors for email security can expose an organization to significant coverage gaps that could be exploited by malware such as the Bofra worm.*

---

the source of inbound emails to DNSBLs, removing spam or virus-infected messages early on in the filtering process. At the same time, the volume of traffic is monitored, with any big spikes in activity taken as a warning of either virus outbreaks or new spam campaigns.

Despite being a useful approach to predicting large-scale outbreaks of email-borne virus variants and spam campaigns, traffic profiling is diminishing in effectiveness for three main reasons.

- 1 The effectiveness of reputation filters can be reduced if spammers and virus writers use zombie networks.
- 2 Relying on traffic spikes to predict outbreaks is not as effective as it once was due to the increasing use of rate-limited attacks, in which the volume of email is restricted in an attempt to stay beneath the radar of security solutions.

---

*Traffic profiling is diminishing in effectiveness as many attacks attempt to stay beneath the radar of security solutions.*

---

- 3 Leading anti-virus and anti-spam engines automatically detect variants of spam campaigns or virus families, providing a more deterministic approach to protection.

## The IT challenge

Increasing vulnerability to the growing number of threats has created correspondingly greater challenges for IT departments in terms of protecting the business network and confidential information, and defending the organization's reputation as a sender.

There are three key IT criteria which a good email protection solution needs to address:

- **Securing multiple points of vulnerability** – ensuring that the workgroup and endpoint defenses work in tandem with the gateway solution.
- **Maintaining system continuity** – minimizing the disruption caused by virus and spam false positives and decreasing the number of alerts or “fire drill” incidents caused by email-borne virus variants attacking the network.
- **Stabilizing administration requirements** – enforcing the business's baseline email security policy to protect confidential information and intellectual property effectively, and managing and controlling resources automatically.

## Sophos PureMessage – meeting the challenge

Sophos rises to the new challenges created by email, providing 24-hour, multi-tier protection against viruses, spyware and spam, and preventing email policy abuse.

### Integrated threat management: securing multiple points of vulnerability

All vulnerable points in the email architecture are protected, from the perimeter through to the endpoint. PureMessage's anti-virus, anti-spam and policy enforcement capabilities at the gateway, email server and workgroup levels are complemented at the endpoint by Sophos Anti-Virus.

### Reliable protection: maintaining system continuity

Sophos PureMessage's reliability in detecting viruses and spam and its high performance capabilities enable IT departments to support the business goal of maintaining system continuity. Genotype™ technology proactively protects the network against fast-developing viruses and new and randomized variants of spam campaigns even before specific updates are available. Genotype technology is used alongside other, more conventional, anti-virus and anti-spam techniques, all of which are used by experts in SophosLabs™ – a global network of threat analysis centers – to provide follow-the-sun protection.<sup>2</sup> The high level of protection against spam and malware provided by PureMessage for UNIX and PureMessage for Windows at the gateway is matched by that of PureMessage for Exchange, which checks the email stores and all traffic passing through the mail server to prevent the internal spread of viruses and spyware.

### Easy to manage: stabilizing administration requirements

PureMessage includes automated administration tools that easily handle and adapt to the mounting requirements as networks become larger and more complex. Its flexibility and scalability mean that it can be easily integrated into any organizational environment.

---

*“The clear king of email policy is Sophos PureMessage...no other product comes close to this functionality.”*

Network World, December 2004

---

In addition, PureMessage for UNIX is standards-based, and supports common Mail Transfer Agents as well as LDAP systems and Active Directory. Its centralized quarantine administration enables the management of enterprise-wide protection from a single point.

Powerful content scanning, message routing and recipient lists are adjustable according to the requirements of even the most complex of organizations, enabling businesses to protect sensitive information such as intellectual property or customer/client data.

### Sophos service

PureMessage is backed up by 24-hour technical support and round-the-clock virus, spam and spyware research in SophosLabs. In addition, Sophos ZombieAlert™ Service can help organizations identify systems on their networks that have been infected and are sending spam. Sophos PhishAlert™ Service provides organizations with early awareness of phishing attacks that hijack their brand or identity.

### Summary

One of the primary weaknesses in the way in which most organizations approach email security is their failure to see it as a multi-tier challenge. Addressing all the vulnerabilities is a hugely complex task for IT professionals, especially given the array of point solutions typically deployed around most organization's email systems.

Sophos PureMessage protects all the key points of vulnerability at the corporate gateway and workgroup email servers, and works with Sophos Anti-Virus at the endpoint to provide consolidated protection across the email infrastructure. Combined with our round-the-clock support services and backed up by the expertise in SophosLabs, PureMessage is the ideal solution for email security in an increasingly complex threat environment.

### About Sophos

Sophos is the world leader in integrated threat management solutions purpose-built for business, education and government. Our reliably engineered, easy-to-operate products protect over 35 million users in over 150 countries. Through 20 years' experience, combined in-house anti-virus and anti-spam expertise, and a global network of threat analysis centers, we respond rapidly to emerging threats – no matter how complex – and achieve the highest levels of customer satisfaction in the industry.

### Sources

- 1 Mind the gap: the integrated multi-tier solution to malicious content, Sophos white paper, July 2005, [www.sophos.com/virusinfo/whitepapers](http://www.sophos.com/virusinfo/whitepapers)
- 2 SophosLabs: integrating day-zero protection in a rapidly changing threatscape, Sophos white paper, June 2005, [www.sophos.com/virusinfo/whitepapers](http://www.sophos.com/virusinfo/whitepapers)